UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/642,617	08/17/2000	David Platt	TIVO0043	6921

7590 04/09/2004

HICKMAN PALERMO TROUNG & BECKLER LLP
1600 Willow Street
San Jose, CA 95125-5106

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	5

DATE MAILED: 04/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/642,617	PLATT, DAVID	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the application filed on 02/04/2004. Claims 1 – 26 were received for consideration. No preliminary amendments to the claims were filed. Claims 1 – 26 are currently being considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

2. Claims 1 and 14 are rejected under 35 U.S.C. 102(b) as being anticipated by Poisner (U.S. Patent No: 6,108,785).

Regarding Claim 1, Poisner teaches and describes a method for providing access between a first party and a second party (Column 1 lines 56 – 65), said method comprising the steps of:

generating a challenge value and a lock value at said first party (Column 2 lines 14 – 18);

transmitting said challenge to said second party (Column 2 lines 14 – 18);

generating a response value from said second party (Column 3 lines 56 – 65);

transmitting said response value to said first party (Column 3 lines 48 – 65); and

validating said response value by said first party (Column 3 lines 64 – 65).

Regarding Claim 14, Poisner teaches and describes an apparatus for providing access between a first party and a second party (Column 1 lines 56 – 65), said apparatus comprising:

means for generating a challenge value and a lock value at said first party (Column 2 lines 14 – 18);

means for transmitting said challenge to said second party (Column 2 lines 14 – 18);

means for generating a response value from said second party (Column 3 lines 56 – 65);

means for transmitting said response value to said first party (Column 3 lines 48 – 65); and

means for validating said response value by said first party (Column 3 lines 64 – 65).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 2, 3, 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Poisner et al (U S Patent 5,596,739) in view of Bensimon et al. (U S. Patent No. 5,533,125).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said first party is a disk drive and said second party is a key device (Poisner Fig.1 #180, #120, #170, #140, Column 2 lines 66 – Column 3 line 6 and Lines 42 - 58). Poisner does not teach a method for providing access between a first party and a second party, wherein said first party is a disk drive and said second party is a host computer. However Bensimon discloses providing access between a first party and a second party, wherein said first party is a disk drive and a second party is a host computer (Bensimon Column 2 lines 63 – Column 3 line 9). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to

implement a method for providing access between a disk drive and a host computer by combining the teachings of Poisner and Bensimon to prevent unauthorized use of a disk drive as taught by Poisner and Bensimon by the host computer as taught by Bensimon. The motivation would have been to prevent the computer system from reading from, or writing to, the disk drive without matching the challenge value from the disk drive to the response value from the computer system.

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Poisner teaches and describes an apparatus for providing access between a first party and a second party, wherein said first party is a disk drive and said second party is a key device (Poisner Fig.1 #180, #120, #170, #140, Column 2 lines 66 – Column 3 line 6 and Lines 42 - 58). Poisner does not teach a method for providing access between a first party and a second party, wherein said first party is a disk drive and said second party is a host computer. However Bensimon discloses providing access between a first party and a second party, wherein said first party is a disk drive and a second party is a host computer (Bensimon Column 2 lines 63 – Column 3 line 9). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a method for providing access between a disk drive and a host computer by combining the teachings of Poisner and Bensimon to prevent unauthorized use of a disk drive as taught by Poisner and Bensimon by the host computer as taught by Bensimon. The motivation would have been to prevent the computer system from reading from, or

writing to, the disk drive without matching the challenge value from the disk drive to the response value from the computer system.

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said disk drive is locked when not accessed (Column 5 lines 16 – 39).

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Poisner teaches and describes an apparatus for providing access between a first party and a second party, wherein said disk drive is locked when not accessed (Column 5 lines 16 – 39).

4. Claims 4 – 13 and 17 – 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Poisner et al (U S Patent 5,596,739) in view of Gillespie et al. (U S. Patent No. 5,657,475) and further in view of Van Oorschot et al. (U S. Patent No. 5,850,443).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said challenge value and said lock

value further includes the step of using logic to generate input data by applying complex algorithm (Poisner Column 3 lines 61 – 67). Bensimon discloses the disk drive to include a password security feature at the device level in that the disk drive cannot be used in any computer system unless the thief also knows the password. (Bensiomn Column 4 lines 45 – 56). Even when taken together, Poisner and Bensimon do not disclose the step of using 512 bits for said challenge value and using 512 bits for said lock value. However, Van Oorschot discloses a method and a system for establishing shared secret keys to allow authentication between two parties and the advantages of using 512 bits for said challenge value and using 512 bits for lock value (Van Oorschot Column 5 lines 60 – Column 6 line 55 and Column 7 lines 20 – 36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a method for providing access between a disk drive and a host computer by combining the teachings of Poisner, Bensimon and Van Oorschot to prevent unauthorized use of a disk drive as taught by Poisner and Bensimon by the host computer as taught by Bensimon and using 512 bits for challenge value and lock value as taught by Van Oorschot. The motivation would have been to prevent the computer system from reading from, or writing to, the disk drive without matching the challenge value from the disk drive to the response value from the computer system and to prevent determination of the algorithm by unauthorized users.

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Poisner teaches and describes an apparatus for providing access between a first party and a

second party, wherein said means for generating a said challenge value and said lock value further includes the step of using logic to generate input data by applying complex algorithm (Column 3 lines 61 – 67). Bensimon discloses the disk drive to include a password security feature at the device level in that the disk drive cannot be used in any computer system unless the thief also knows the password. (Bensiomn Column 4 lines 45 – 56). Even when taken together, Poisner and Bensimon do not disclose the step of using 512 bits for said challenge value and using 512 bits for said lock value. However, Van Oorschot discloses a method and a system for establishing shared secret keys to allow authentication between two parties and the advantages of using 512 bits for said challenge value and using 512 bits for lock value (Van Oorschot Column 5 lines 60 – Column 6 line 55 and Column 7 lines 20 – 36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a method for providing access between a disk drive and a host computer by combining the teachings of Poisner, Bensimon and Van Oorschot to prevent unauthorized use of a disk drive as taught by Poisner and Bensimon by the host computer as taught by Bensimon and using 512 bits for challenge value and lock value as taught by Van Oorschot. The motivation would have been to prevent the computer system from reading from, or writing to, the disk drive without matching the challenge value from the disk drive to the response value from the computer system and to prevent determination of the algorithm by unauthorized users.

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said challenge value and said lock value further includes the step of randomly generating each said challenge value (Poisner Column 3 lines 61 – 67).

Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, Poisner teaches and describes an apparatus for providing access between a first party and a second party, wherein said means for generating a said challenge value and said lock value further includes the step of randomly generating each said challenge value (Poisner Column 3 lines 61 – 67).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said challenge value and said lock value further includes the step of using a disk drive controller to generate said challenge value (Poisner Fig.1 #165, Column 4 lines 60 – 65; Bensimon Column 4 lines 62 – 67).

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Poisner teaches and describes an apparatus for providing access between a first party and a second party, wherein said means for generating a said challenge value and said lock

value further includes the step of using a disk drive controller to generate said challenge value (Poisner Fig.1 #165, Column 4 lines 60 – 65; Bensimon Column 4 lines 62 – 67).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said response value further includes the step of processing the challenge value and logic value (Poisner Column 4 lines 9 – 16 and lines). Van Oorschot discloses the step of using an exclusive OR (XOR) to combine the said challenge and said lock values (Van Oorschot Column 6 lines 56 – 60 and Column 7 lines 1 – 19).

Claim 20 is rejected as applied above in rejecting claim 19. Furthermore, Poisner teaches and describes an apparatus for providing access between a first party and a second party, wherein said means for generating a said response value further includes the step of processing the challenge value and logic value (Poisner Column 4 lines 9 – 16 and lines). Van Oorschot discloses the step of using an exclusive OR (XOR) to combine the said challenge and said lock values (Van Oorschot Column 6 lines 56 – 60 and Column 7 lines 1 – 19).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Van Oorschot teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said response value further

includes the step of using 160 bits for said response value (Van Oorschot Column 6 lines 50 – 55).

Claim 21 is rejected as applied above in rejecting claim 20. Furthermore, Poisner teaches and describes an apparatus for providing access between a first party and a second party, wherein said means for generating a said response value further includes the step of using 160 bits for said response value (Van Oorschot Column 6 lines 50 – 55).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said response value further includes the step of using a cryptography circuit to generate said response value (Poisner Column 4 lines 9 – 26).

Claim 22 is rejected as applied above in rejecting claim 21. Furthermore, Poisner teaches and describes an apparatus for providing access between a first party and a second party, wherein said means for generating a said response value further includes a cryptography circuit to generate said response value (Poisner Column 4 lines 9 – 26).

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said response value further includes the

step of using an algorithm to generate said response value (Poisner Column 3 lines 42 – 61).

Claim 23 is rejected as applied above in rejecting claim 22. Furthermore, Poisner teaches and describes an apparatus for providing access between a first party and a second party, wherein said means for generating a said response value further includes the step of using an algorithm to generate said response value (Poisner Column 3 lines 42 – 61).

Claim 11 is rejected as applied above in rejecting claim 10. Furthermore, Van Oorschot teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said response value further includes the step of using a secure hash algorithm to generate said response value (Van Oorschot Column 6 lines 49 – 55).

Claim 24 is rejected as applied above in rejecting claim 23. Furthermore, Van Oorschot teaches and describes an apparatus for providing access between a first party and a second party, wherein said step of generating a said response value further includes the step of using a secure hash algorithm to generate said response value (Van Oorschot Column 6 lines 49 – 55).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of validating said response value further includes the step of said disk drive controller receiving the challenge and lock values, computing a duplicate response value by performing a duplicate algorithm, and comparing the original said response value to the duplicate said response value (Poisner Column 3 lines 60 – 67). Poisner does not teach computing a duplicate response value by performing a duplicate said secure hash algorithm. Van Oorschot discloses computing a duplicate response value by performing a duplicate said secure hash algorithm (Van Oorschot Column 6 lines 49 – 55).

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Poisner teaches and describes an apparatus for providing access between a first party and a second party, wherein said means for validating said response value further includes the step of said disk drive controller receiving the challenge and lock values, computing a duplicate response value by performing a duplicate said algorithm, and comparing the original said response value to the duplicate said response value (Poisner Column 3 lines 60 – 67). Poisner does not teach computing a duplicate response value by performing a duplicate said secure hash algorithm. Van Oorschot discloses computing a duplicate response value by performing a duplicate said secure hash algorithm (Van Oorschot Column 6 lines 49 – 55).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of validating said response value further includes the step of unlocking the disk drive if the response and duplicate response values match (Poisner Column 3 lines 65 – Column 4 line 25, Column 5 lines 12 – 37 and Column 6 lines 20 – 40).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Poisner teaches and describes an apparatus for providing access between a first party and a second party, wherein said means for validating said response value further includes the step of unlocking the disk drive if the response and duplicate response values match (Poisner Column 3 lines 65 – Column 4 line 25, Column 5 lines 12 – 37 and Column 6 lines 20 – 40).

Conclusion

6. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231 **or faxed to:** (703) 872-9306 for all formal communications.

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 703-305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Pramila Parthasarathy
April 02, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100